

ABSTRACT

A method for enabling secure communication over a network is described. This method employs a public/private key encryption/decryption algorithm through a secure communication device. The communication device is designated as capable of secure communication when it is equipped with the necessary electronics to perform the encryption and decryption, as one embodiment is described herein. The encryption/decryption method utilized by embodiments of the invention can be incorporated into the modification of, conventional communication terminals such as a telephone. Such modifications are comprised of, but not limited to, the addition of components (refer to Figure 1) capable of converting voice signals to digital signals and vice versa. The communication terminal may also include, for example, a specially designed ASIC processor and/or software configured to encrypt and decrypt data. In one embodiment of the invention measures are taken to limit accessibility to the keys utilized to perform encryption/decryption.